



Legislative Audit Workshop

Cybersecurity in the Year 2020

Jim Edman Chief Information Security Officer
Miguel Penaranda Deputy CISO

5/19/2020



Critical Cyber Security Recommendations

Backup Your Data

- Decouple from live system after backup
- Test Restoring It

Apply Automatic Updates & Patches

- Windows, Adobe, Java, Business Apps

Education & Training

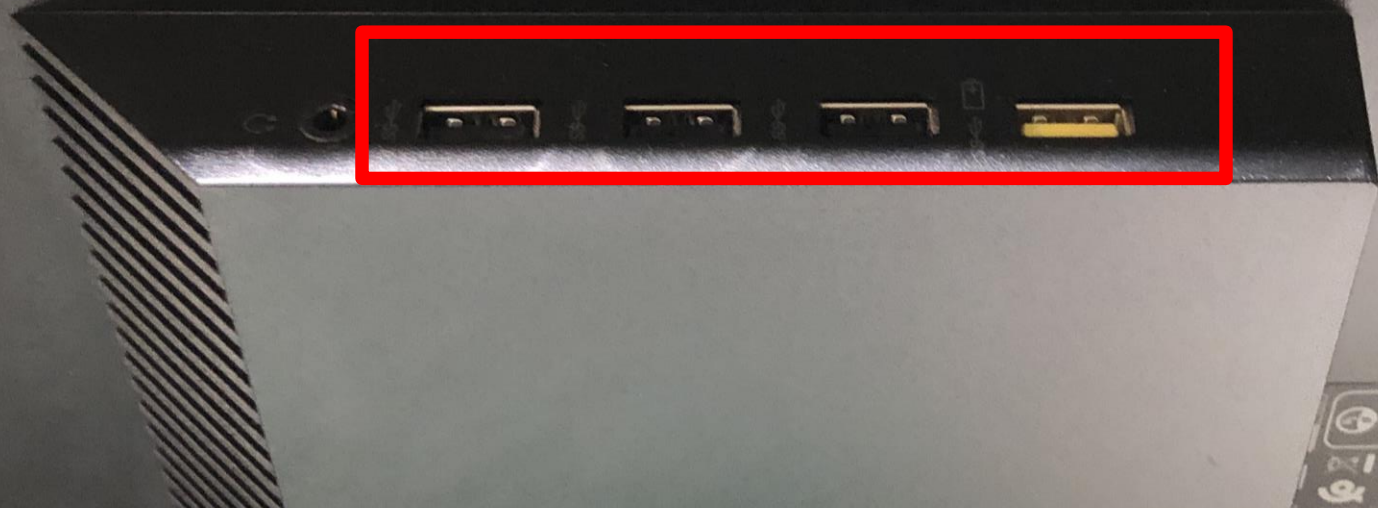
- Cybersecurity class
- Business Email Compromise
- Remote Work

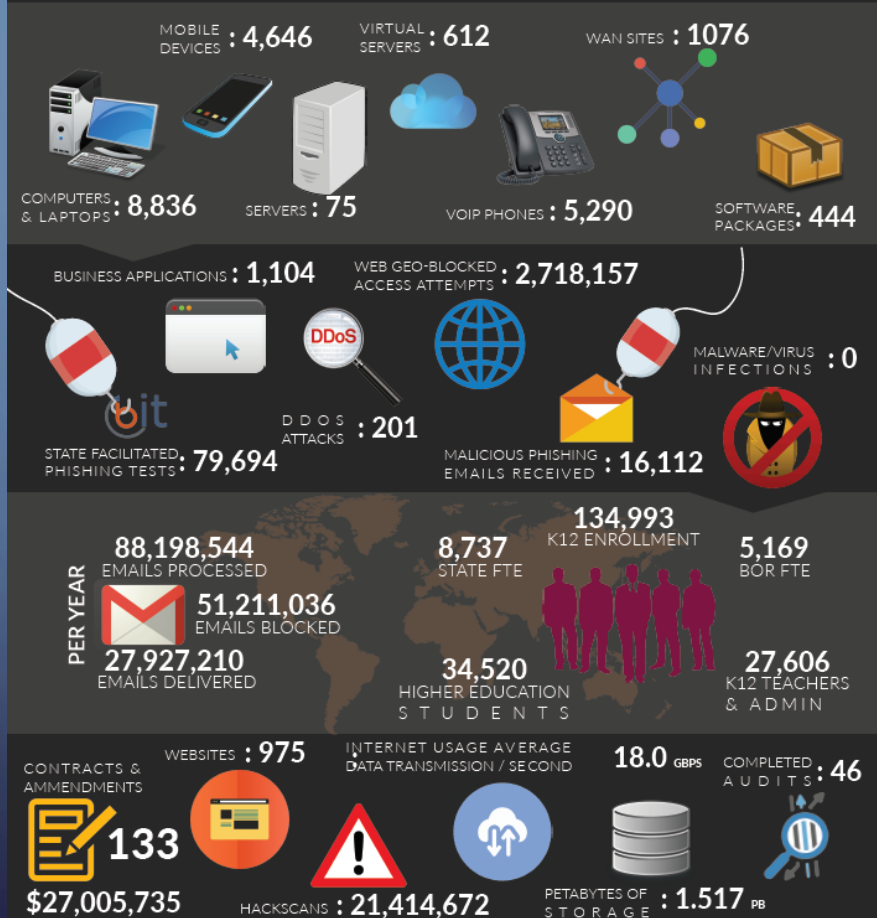
User Level privileges

CYBERSECURITY COMPROMISE EXAMPLES

- Texas School District **\$2.3M** (Vendor Impersonation)
- City of Baltimore, MD (3) **\$18.2M** (\$76K ask - Ransomware)
- City of Atlanta, GA **\$17M** (\$25K ask - Ransomware)
- 22 Texas Counties **\$12M** (\$2.5M ask - Ransomware)
- City of Sioux Falls **\$???** (Vendor Impersonation)
- Yankton, SD School District (Malicious)
- SD School Teacher (Direct Deposit)
- Iowa Retirement Benefits Fraud (Direct Deposit)

Not all security is social engineering or complicated software hacks.





DDN Support and K-12 Data Center Services and Support



K12 Data Center



Foundational Services



DDN Support



129,772
Students

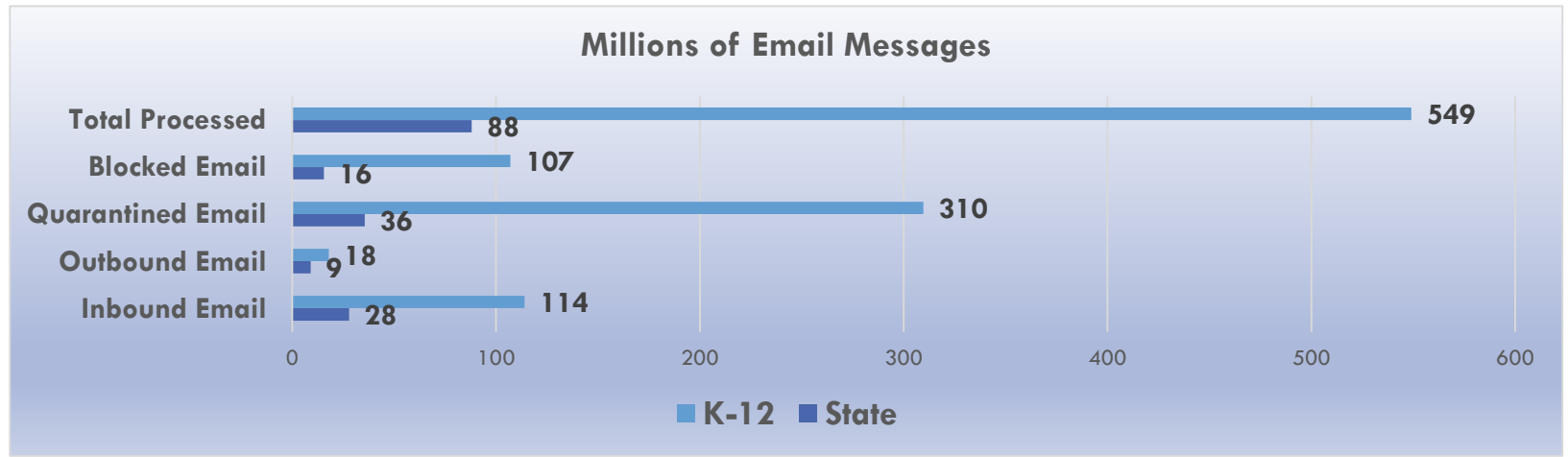
9,867
Teachers &
Administrators

150
Public Districts

125,471
User Accounts

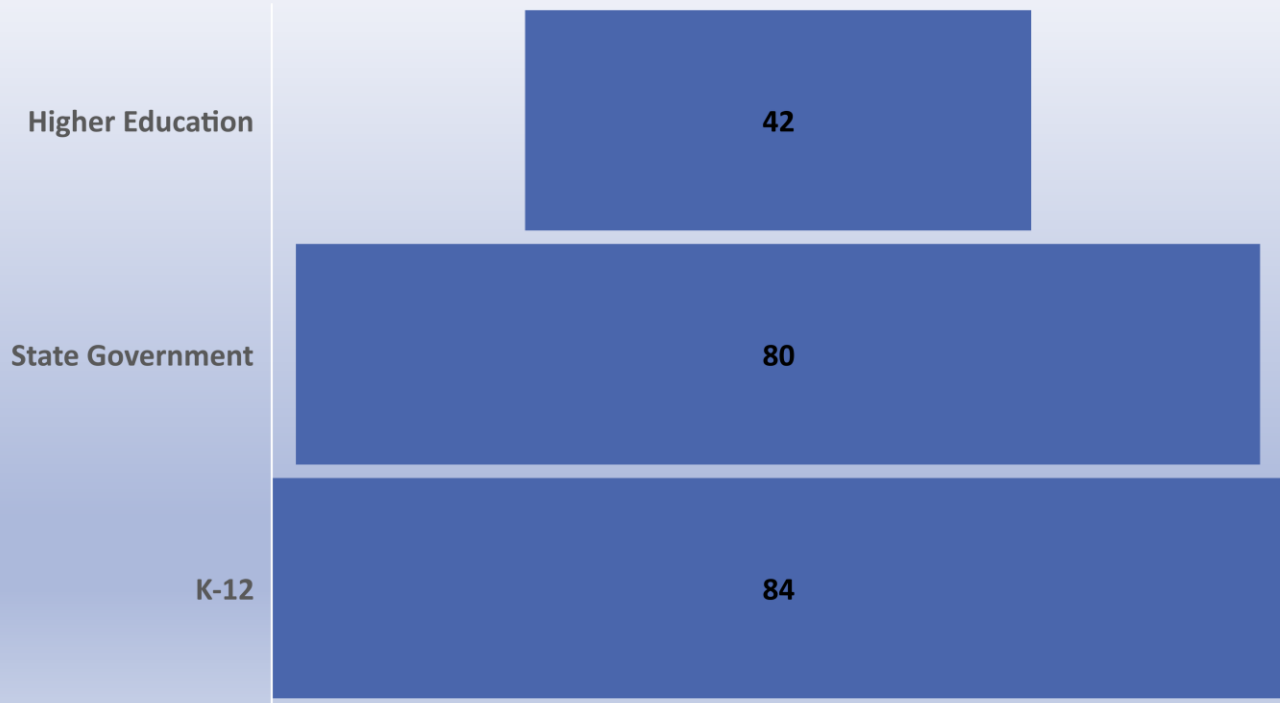
2,914
Distance Learning
Classes

4,554
E-Learning
Classes



CYBERSECURITY STATS

Distributed Denial of Service Network Attacks

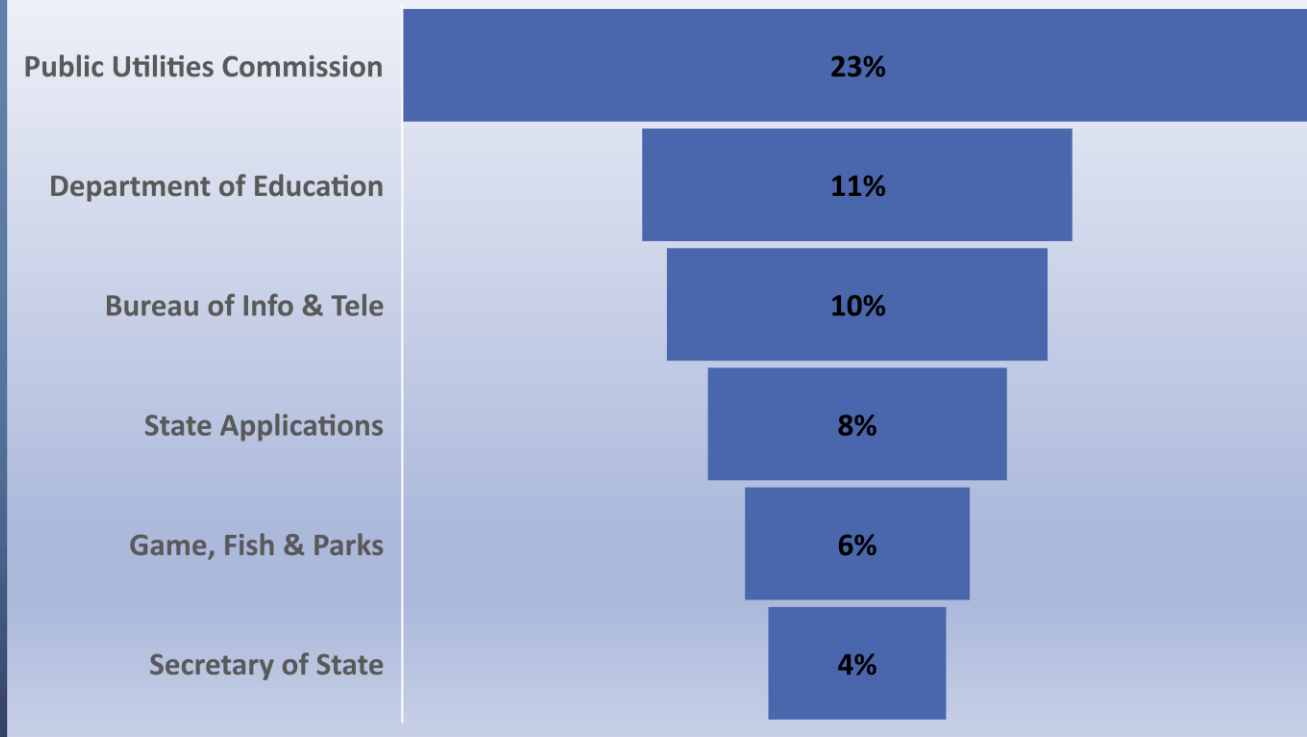


A denial-of-service attack is a cyber-attack in which the cyber threat actor seeks to make an Internet server or website unavailable to its users by temporarily or indefinitely disrupting services.

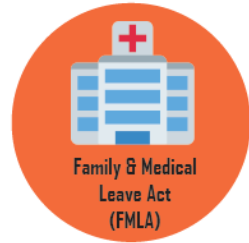
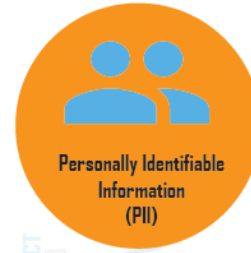
A digital “traffic jam”.

CYBERSECURITY STATS

Agency Web Sites Attacked Most Frequently



CYBERSECURITY STATS



Why CYBERSECURITY is Important



Types of Threat Actors

Advanced Persistence Threat

- Nation State funded threat actors. China, Iran, North Korea, Russia

Cybercriminals

- Groups and individuals that either target or utilize opportunistic methods based on system vulnerabilities

Criminal Hackers

- Hackers for hire; typically motivated by financial gain
- Identity theft and healthcare fraud are their main targets

Terrorists

- Politically driven groups and individuals
- Utilize target or opportunistic methods with system vulnerabilities

Employees

- Malcontents
- Spies

Types of Attacks

Social
Engineering

Phishing

Ransomware

Credential
Harvesting

Application
Attacks

Supply
Chain

Physical
Security

Denial of
Service
Attacks

Destruction

Virus &
Malware

Resource
Usage

Insider
Threat

RANSOMWARE

A type of malicious software designed to block access to a computer system until a sum of money is paid.

Common names of ransomware:

Bad Rabbit

CryptoLocker

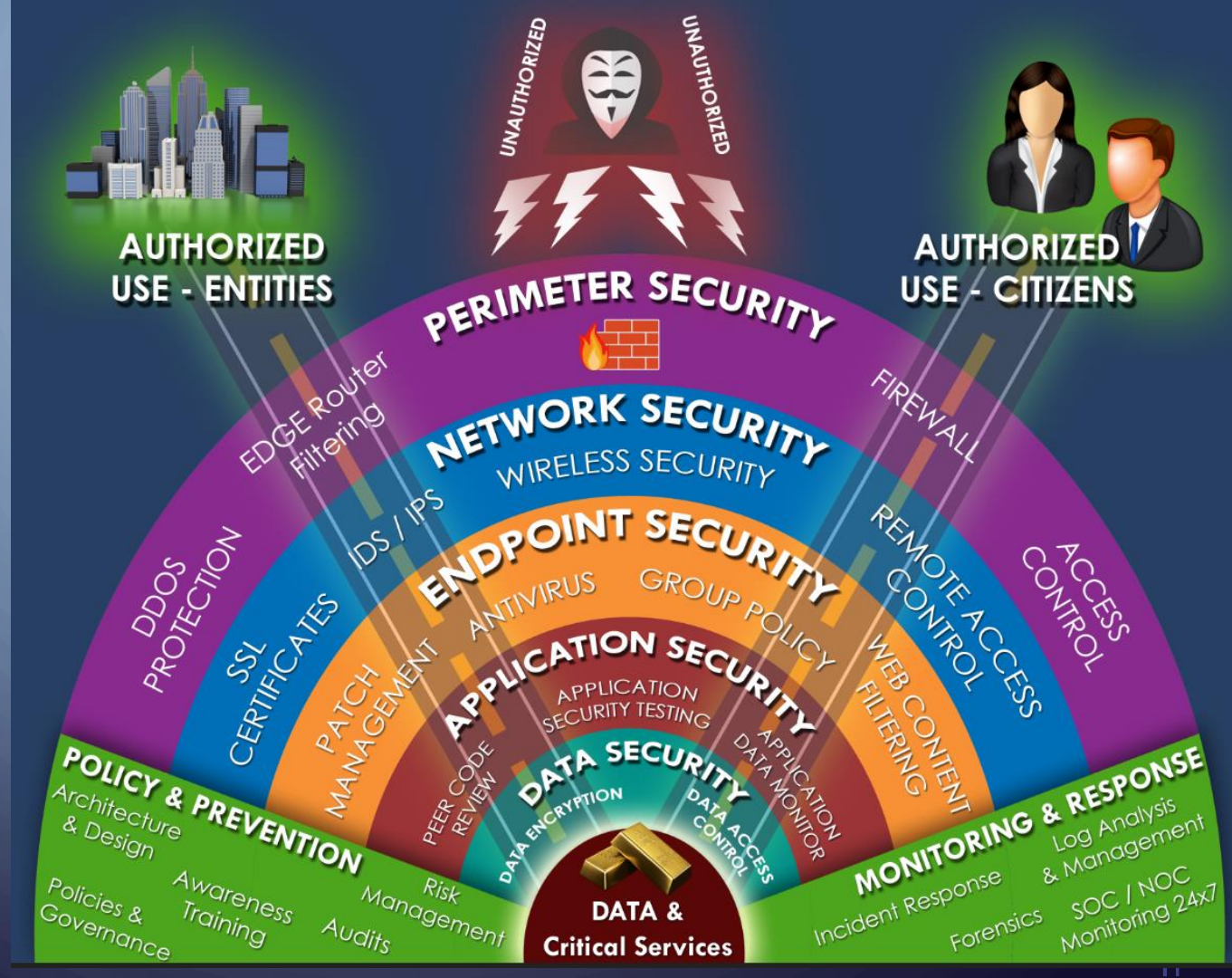
CrytpoWall

Ryuk

WannaCry

South Dakota

Cybersecurity Infrastructure



Average amount time
hackers are in a network
before being discovered:





Business Email Compromise Scams

Vendor
Impersonation

Payroll Direct
Deposit

Account
Credentials
(Username &
password)

Wire Transfer
Request

Vendor Purchase
Order request

Real
Estate/Escrow
Fund Transfer

Malware Delivery

Gift Cards

Date:
FROM: Vendor
TO: Purchasing@<state>.gov
SUBJECT: Account Change

Good morning. We are in the process of changing our accounts. Please remit payment to <new account>.

State of South Dakota
BFM-0001 (V03/201907)



SEND TO THE STATE AGENCY
YOU SEND INVOICES
DO NOT send to IRS

Substitute **W-9**

Taxpayer Identification Number (TIN) Verification

Print or Type
Please see attachment or reverse for complete instructions.
This form can be made available in alternative formats to qualified individuals upon request.

Optional Direct Deposit Information			
Your Bank Account Number	<input type="checkbox"/> Checking <input type="checkbox"/> Savings	Bank Routing Number (9-digit ABA #)	Name on Bank Account
THIS IS A: <input type="checkbox"/> new direct deposit <input type="checkbox"/> change of existing (providing old banking information required to change existing)			
Old Bank Account Number	Old Routing Number (9-digit ABA #)	You must provide the previous banking information to make a change.	

Could this happen in SD?

RECONNAISSANCE

- Open.SD.Gov: Vendors, \$\$\$, Dates, Contracts, Contacts
- Internet: Employer Identification Number (EIN), SSNs
- Identify State employees: Online phone book, news, web sites

ENGAGEMENT

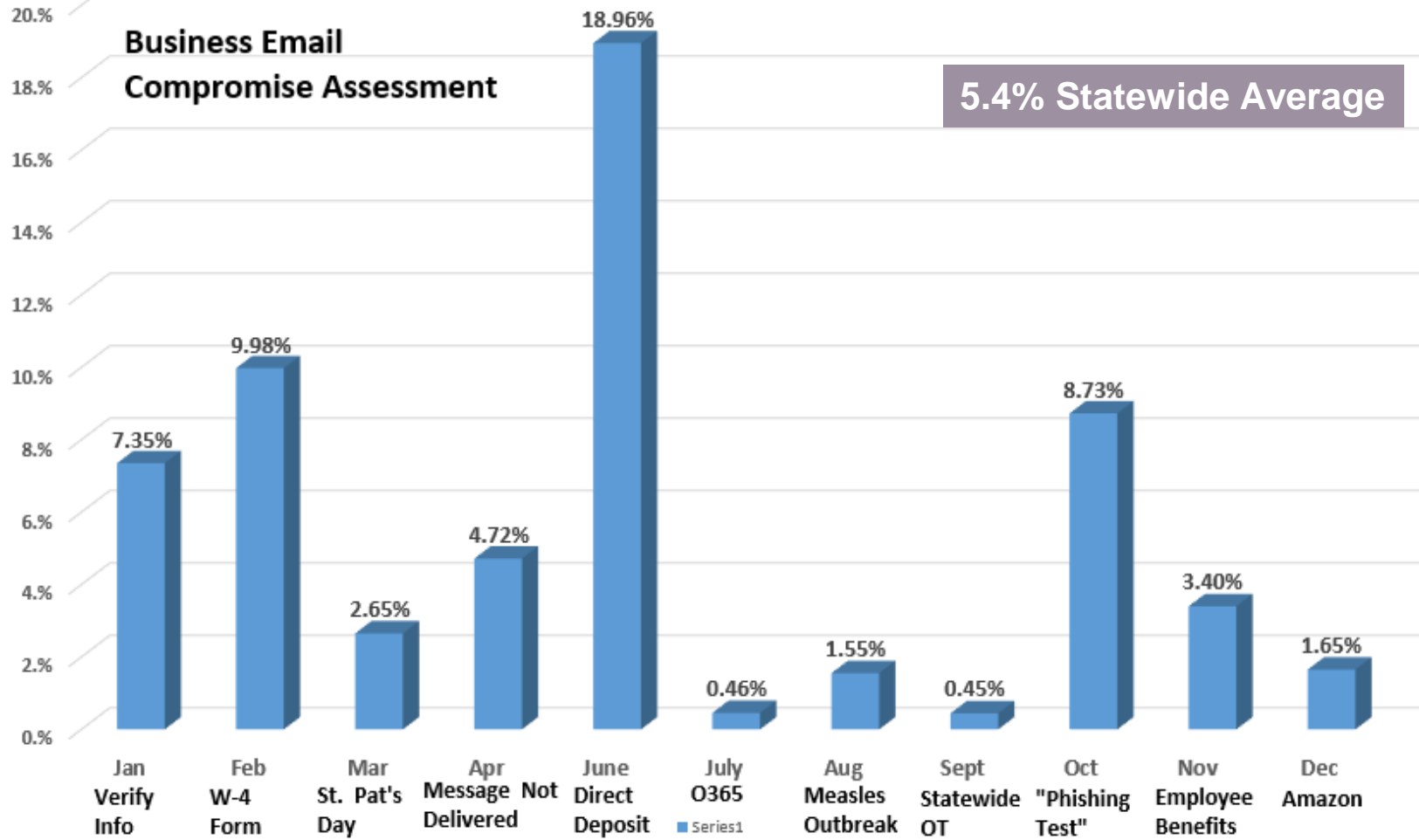
- Email exchanges
- “Can you help me?”


ACTION

- Update Systems
- Process Invoices, Payroll, etc.
- Divert Payments, Direct Deposits, etc.

Business Email Compromise Assessment

5.4% Statewide Average





Slowing down isn't just for children

When reading through
your email, **STOP** and
THINK before you click

CRITICAL EMAIL STEPS

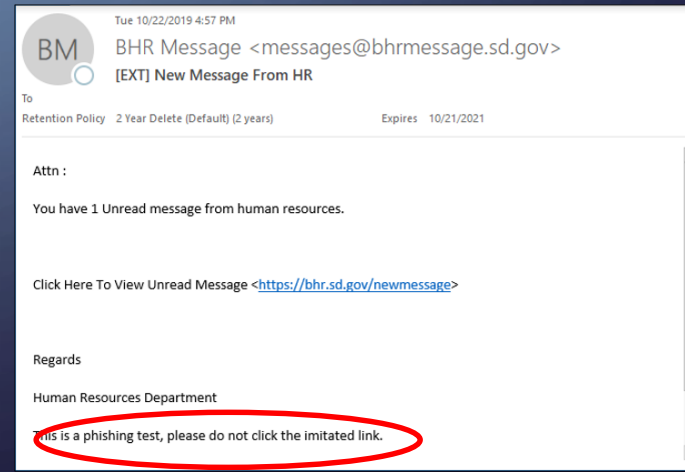
1. Reading is Fundamental
2. Look at the From: Name
3. Look at the From: Email Address. Name AND Address.
4. Subject: Familiar?
5. Message
 - a. Spelling, Grammar & Content
 - b. Don't be swayed by branding
 - c. Hover over links
 - d. Attachments
5. Computer vs Mobile
6. Junk Mail Options

Reading
Is Fundamental

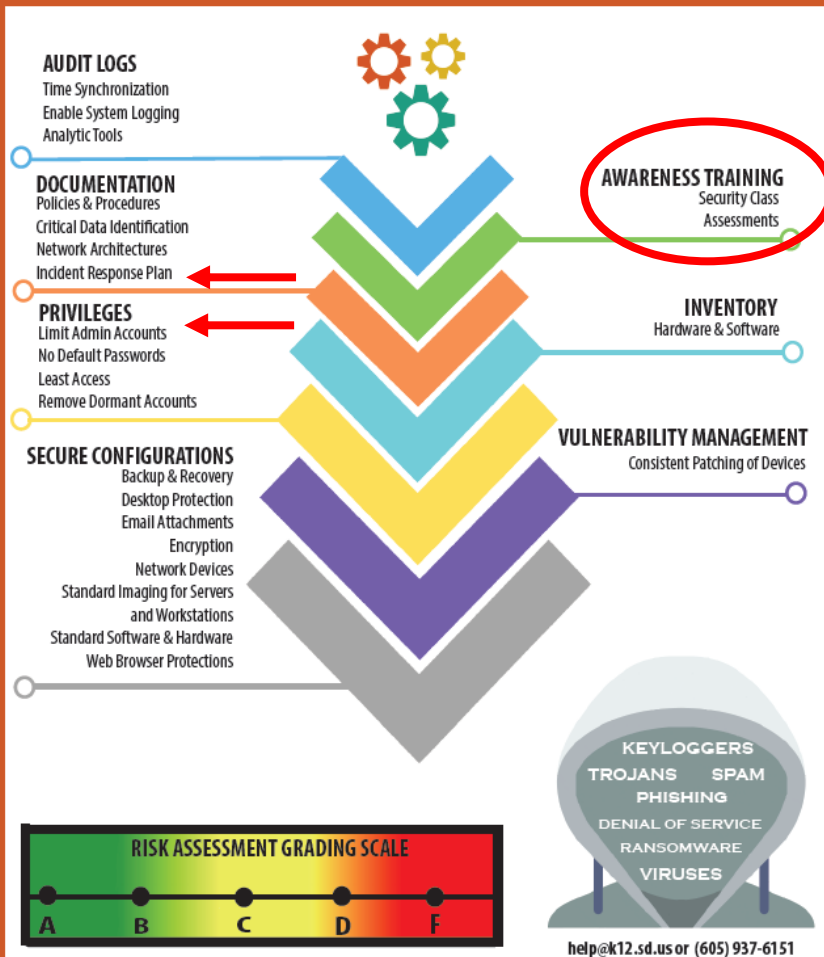
CAUTION
SLOW DOWN

WHEN READING EMAIL!

DON'T BE PHISHED



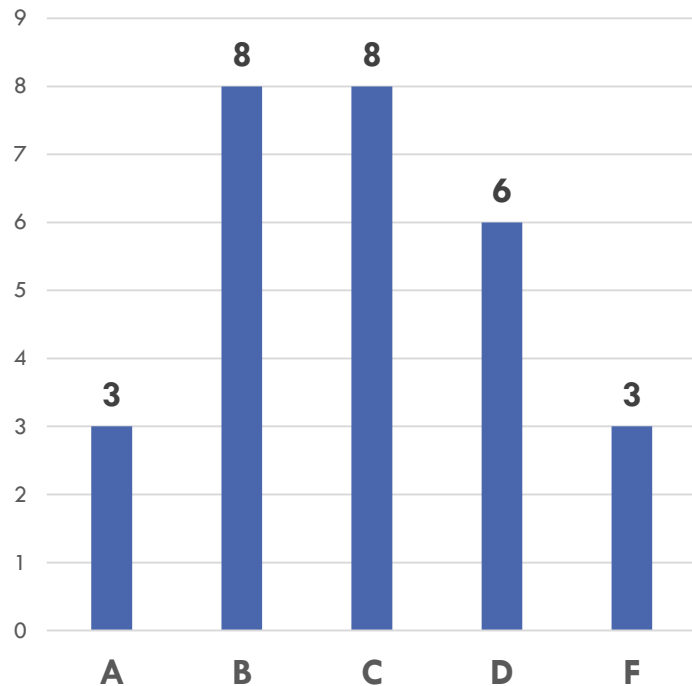
K-12 CYBERSECURITY RISK ASSESSMENT



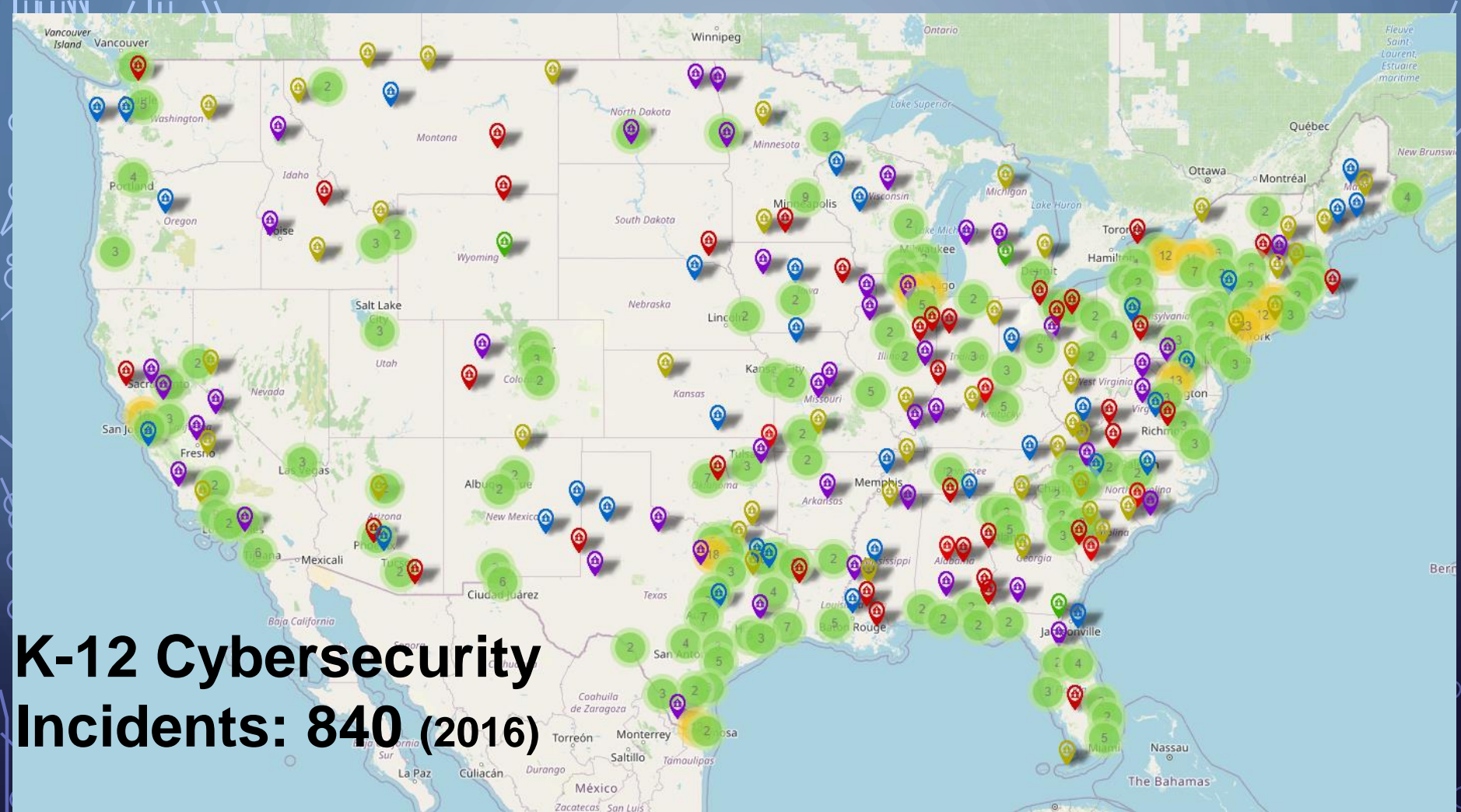
K-12 Cybersecurity Risk Assessment

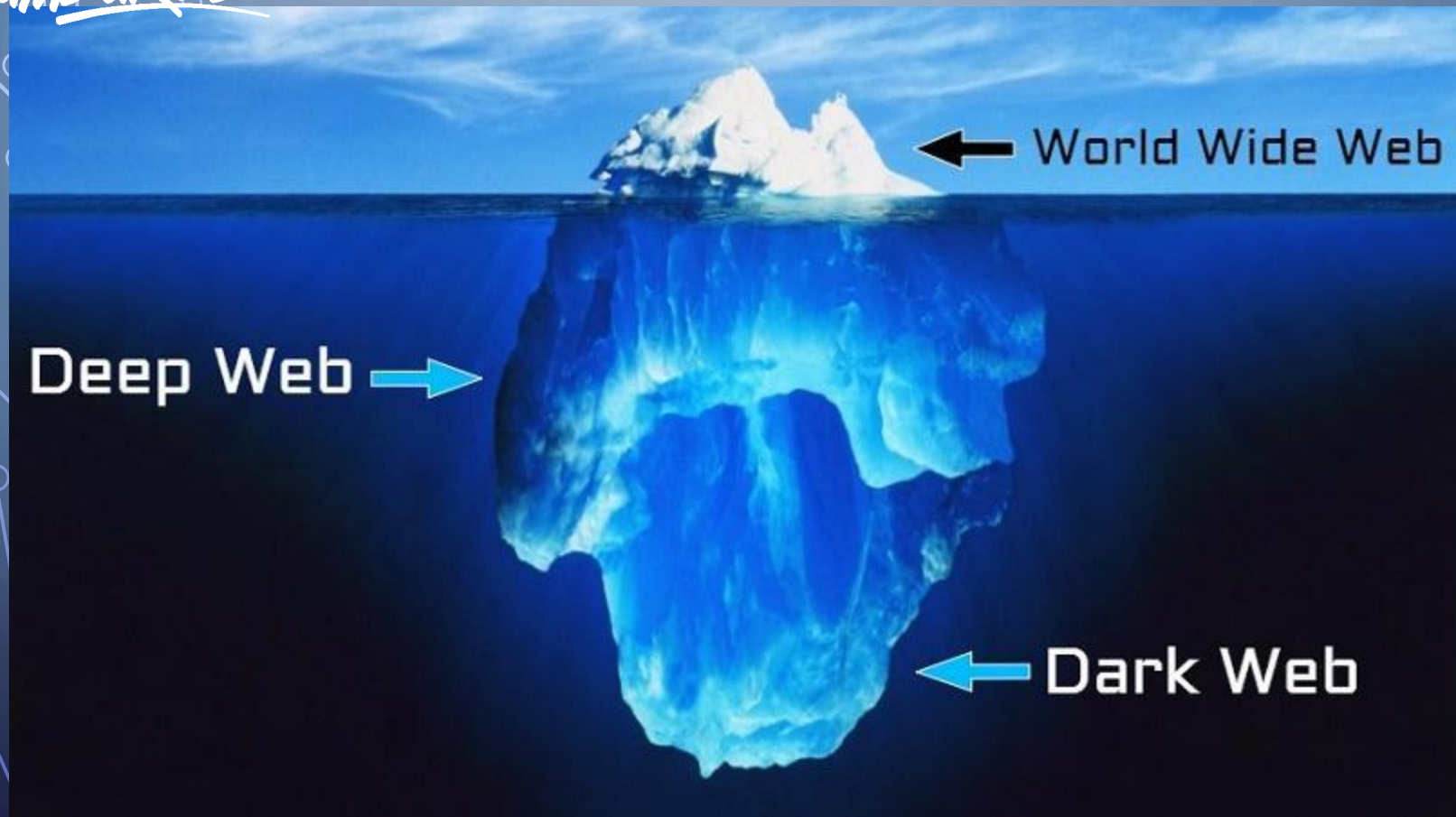
- Based on industry standard
CIS Top 20 Controls

SCHOOL ASSESSMENT PERFORMANCE



K-12 Cybersecurity Incidents: 840 (2016)







CRYSTAL METH 7gram

฿ 1.61

BUY



COKE From PERU 93%, 7 gram,
FINALIZE EARLY

฿ 2.37

BUY



COKE From PERU 93%, 3 gram

฿ 1.27

BUY



Crystal Meth - 2g

฿ 0.85

BUY

SHOW STIMULANTS CATEGORY



LSD Anonymous 140µg, 50 blotters

฿ 1.1

BUY



1 OZ Super Stong Mushrooms

฿ 0.59

BUY



1oz Cubensis Mushrooms

฿ 0.61

BUY



!! SPECIAL OFFER 1oz DRY PSILOCYBIN
CUBENSIS SHROOMS!!

฿ 0.42

BUY

Critical Cyber Security Recommendations

Backup Your Data

- Decouple from live system after backup
- Test Restoring It

Apply Automatic Updates & Patches

- Windows, Adobe, Java, Business Apps

Education & Training

- Cybersecurity class
- Business Email Compromise
- Remote Work

User Level privileges

south dakota

